Don't Let Your Data Be Held for Ransom

Use Cisco solutions to help protect your data from ransomware.

Modern solution

- Deploy a secure solution ready to protect against ransomware.
- Deploy a solution that is ready to integrate into the cloud.

Rapid recovery

- Restore operations quickly in the event of a data loss.
- Recover virtual machines by booting directly from the backup data.

Validated backups

- Help ensure that your backup copies are valid and ready for use when you need them.
- Use solution tools to validate backup copies in a sandboxed environment.

Your business could suffer major losses without a plan for handling ransomware. We offer a comprehensive solution

We have all seen the headlines. Businesses brought to a standstill because of malware that has encrypted data. Healthcare organizations, pharmaceuticals companies, financial institutions, automobile manufacturers, shipping companies—all have fallen prey to ransomware. No enterprise is immune, and no area of business is immune. Sometimes attacks can obscure the hackers' real agenda: theft of customer data. This theft can have a dramatic impact on your reputation and your regulatory compliance. You need a comprehensive approach for preventing attacks and for recovering impacted or lost data if an attack succeeds.

Ransomware defense

Ransomware can penetrate an organization's defenses in multiple ways, so reducing the risk of infection requires a layered approach. We use an architectural approach to ransomware defense that strengthens your defenses with detection, visibility, and intelligence. We help you protect everything from beyond your network perimeter to your endpoints anywhere and at any time.

Ransomware recovery

Hackers are now armed with some of the most potent intrusion tools, and there is always a chance that a zero-day attack can pierce even the most formidable defenses. Good backup operations for software and data are essential. But protection against ransomware also requires modern infrastructure and software. The survival of your organization depends on your capability to recover applications and data in the event of an attack. Our storage-intensive servers, along with software from our partners Commvault and Veeam, help your enterprise meet the most demanding recovery requirements.

Ransomware concerns

- Ransomware exploits cost US$1 billion in 2016
- Ransomware-as-a-service platforms are gaining popularity, increasing risk.
- 49 percent of companies suffered at least one ransom incident
- 39 percent experienced a ransomware attack
- 17 percent experienced a ransomware denial-of-service attack

Source: Cisco 2017 Midyear Cybersecurity Report

Keep ransomware out of your network

The first step in our ransomware defense strategy is to prevent malicious content from entering the network. Our solutions protect against Domain Name System (DNS) queries to endpoints, including servers and laptops. Our products are backed by Cisco Talos™, the industry-leading threat intelligence solution dedicated to providing protection before, during, and after cybersecurity attacks.

Our network and endpoint protection solutions deliver layered, integrated defenses that give you immediate visibility into potential threats, and automatically contain threats when they are detected. For example, Cisco TrustSec® software-defined segmentation can keep ransomware contained and unable to threaten other parts of your organization.

Protect your data against all losses

No single product or even a suite of products can protect against every threat. Protecting data with timely, secure backup operations can help ensure a quick return to production after a data loss.

Cisco® security architecture can help protect you against ransomware and a wide range of other possible sources of data loss. Our solutions combine storage-dense Cisco UCS® S-Series Storage Servers with software from leading backup software vendors to give you a solution that delivers modern data protection and is tuned to protect you from ransomware.

Set an appropriate recovery-point objective

A recovery-point objective (RPO) is the most distant point in time from which you are willing to lose data. For more business-critical applications, shorter RPOs are appropriate. For example, an online transaction processing system is at the core of the business, and little data loss is acceptable. For less business-critical applications, longer RPOs may be fine. Individual users, for example, may be able tolerate some data loss without risk to the business and thus can have longer RPOs.

The combination of short RPO and rapidly changing data requires frequent backup operations and results in large amounts of data. You will need high-capacity storage and high network bandwidth to store and transmit frequent backup copies.

Use API-based backups

Some backup strategies for user desktops transfer data to network shares using the same login credentials as the user. This approach puts backups at risk because ransomware seeks out network shares that it can access and encrypt.

Modern backup approaches use APIs to extract data through the

> **"Even ransomware couldn't stop us from recovering from a backup in minutes... We're amazed by what Veeam and the S3260 can do."**

Bendix Søjberg
IT Operations Manager
University College Zealand

Full story

operating system or hypervisor and use different security credentials so that ransomware has little chance of interfering with backup data. This type of approach helps block typical spread paths through network shares and other services accessible with your users' credentials.

Our solutions using Commvault and Veeam software use APIs to obtain backup data for everything from virtual machines to bare-metal servers. The software transfers backup data to Cisco UCS S3260 Storage Servers.

Restore data fast

Because these servers can make large amounts of data available instantly in the event of a data loss, restoration is fast and easy. Virtual machines and virtual desktops can be restored instantly simply by booting from an image on the storage server and migrating the virtual machines back to the cluster. Users can restore individual files through intuitive GUIs, helping reduce the burden on administrators (Figure 1).

Validate backups

Backup copies should be tested regularly to be sure that they are protecting your data as you intend. Our solutions with Veeam and Commvault allow you to boot a backed-up virtual machine in a sandboxed environment so that you can be sure that the restored image performs as you expect.

Use the 3-2-1 rule

The 3-2-1 rule implemented with our data protection solutions

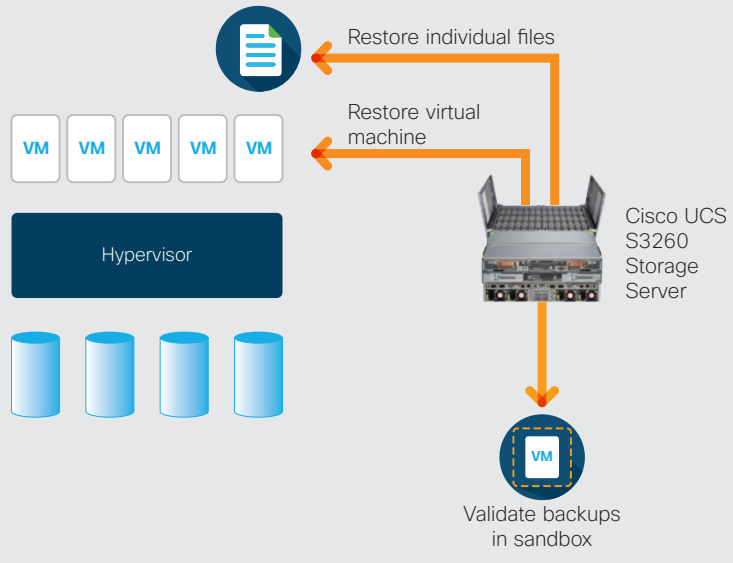

Figure 1 Fast restoration and validated backups are essential to a modern backup strategy

“The big trend has been compliance, governance, disaster recovery, SLAs, RPOs, RTOs, and with Commvault we’ve been able to provide this seamlessly to our customers almost five-9s”

Perry Larson
Senior Technical Advisor
Public Consulting Group
Full story

increases resilience in the event of malware attacks and other failures that result in data loss. This rule consists of the following:

3. Create at least three copies of your data. Make your initial backup copy on your fastest device: for example, your S3260 Storage Server. Then replicate this data to other locations and media (Figure 2).
2. Use at least two types of media. Spinning disks are quickly accessible but can be modified. Tape is a stable, offline backup medium that cannot be overwritten during an attack.
1. Store at least one copy of your data offsite so that in the event of a geographic failure, you have a backup copy that can restore data to a known state.

Choose fast restoration

Our solutions help you restore software and data quickly in the event of a data loss. You can restore an entire virtual machine by booting its image directly from the storage server and migrating it back to the production cluster. Users have the power to restore individual files through an intuitive GUI, reducing the burden on administrators.

Solutions with the Cisco UCS S3260 Storage Server

The Cisco UCS S3260 Storage Server (Figure 3) has the right characteristics to support modern data protection solutions, storing your data quickly and efficiently.

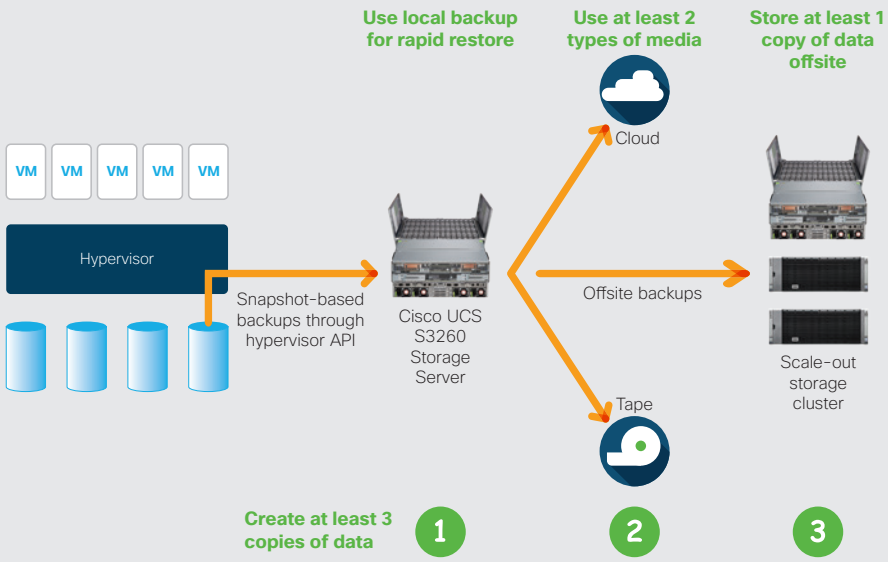

Figure 2 The 1-2-3 rule helps you get the most out of a backup solution

Figure 3 The Cisco UCS S3260 Storage Server configured with 56 disk drives and two computing nodes

The server is a modular, high-density system optimized for storage-intensive workloads It features a 2-node design that gives you the performance and bandwidth of two servers in a single chassis, requiring fewer servers to support your data-protection solution. Each of the server's two nodes hosts dual 40-Gbps connectivity for a total of 160 Gbps—sufficient to support the shortest RPOs. The server hosts up to 600 TB of data, and if that isn't enough, our solutions let you increase capacity further with scale-out configurations. Network bandwidth is essential for data replication, so choosing a solution using the S3260 gives you the speed that you need to support the 3-2-1 rule for safe and secure data protection.

The S3260 server is designed to be modular so that you can update components individually, giving you long-term investment protection. The server also offers low total cost of ownership (TCO), as demonstrated in a direct comparison with Amazon Simple Storage Service (S3). With the S3260, you can achieve 56 percent lower costs and a 13-month break-even point by hosting storage in your own data center.

With local storage costing less than cloud-based storage, our solutions with Commvault and Veeam combined with the S3260 Storage Server offer an excellent choice.

Next steps

We can help you stay ahead of the ransomware problem with the best in network and endpoint security combined with industry-leading backup solutions. With Cisco Services to help you get your solutions up and running quickly, you can make sure that your data can't be held for ransom.

For more information

cisco.com/go/dataprotection

cisco.com/go/ransomware

LE-62601-00 09/17